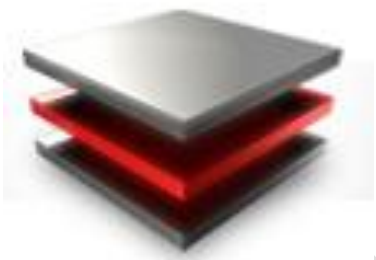
به نام خدا



نویسنده : سینا احمدی (ENCODER)

آدرس ایمیل : ENCODER_ASHIYANE@YAHOO.COM

تاریخ انتشار : 88/10/25

آدرس سایت : HTTP://ASHIYANE.ORG/FORUMS

آشنایی با HASH :

یک هش که به آنCheckSUM، پیام Digest یا اثر انگشت نیز گفته می شود ، فرایندی است که بصورت ریاضی، حجم یک جریان از داده را به یک طول ثابت کاهش می دهد (معمولا" 128 و یا 160 بیت) . عملکرد هش ، مشابه اثرانگشت یک شخص می باشد. اثرانگشت ، پارامتری منحصربفرد به منظور تشخیص هویت افراد بوده و در ادامه با استفاده از آن امکان دستیابی به سایر مشخصات افراد نظیر : رنگ چشم ، قد ، جنسیت و سایر موارد دلخواه ، فراهم می گردد . اکثر توابع هش از لحاظ رمزنگاری دارای عملکردی مشابه توابع رمزنگاری می باشند . در حقیقت ، برخی توابع هش صرفا" تغییرات اندکی را در توابع رمزنگاری ایجاد نموده اند . اکثر عملیات با دریافت یک بلاک از داده شروع و در ادامه با استفاده از یک فرآیند تکرارشونده و بکارگیری یک الگوریتم رمزنگاری ، تغییرات لازم در ارتباط با بیت ها ، اعمال می شود

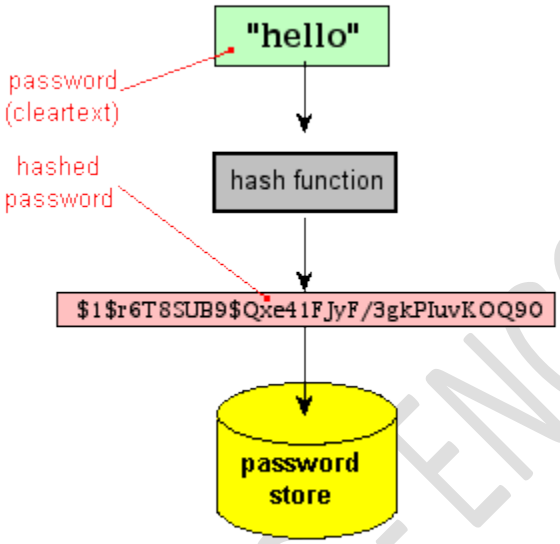
HASH به روایتی دیگر :

هش (Hash, Hash Code, Digest, Message Digest هم نامیده می شود) را می توان به صورت اثر انگشت دیجیتالی یک داده در نظر گرفت. با این روش شما می توانید رشته ای اندازه-ثابت(fixed length) از یک داده به دست آورید که با روش های ریاضی به صورت "یک طرفه" رمزنگاری شده است. کشف رشته اصلی از رشته هش آن (عملیات معکوس) به صورت کارا تقریبا غیر ممکن است. نکته دیگر اینکه هر داده یک رشته هش میباشد شده کاملا منحصر به فرد ایجاد می کند(احتمال یکی شدن رشته های هش دو رشته متفاوت در الگوریتم MD5 یک در 3.402823669209384634633746074317 7e+38!

این خواص ، هش کردن را به روشی کارا و ایده آل برای ذخیره سازی کلمات عبور در برنامه های شما تبدیل می کند. چرا؟ برای این که حتی اگر یک نفوذگر (هکر - HACKER)

بتواند به سیستم و بانک اطلاعاتی شما نفوذ کند و بخشی از اطلاعات شما را به دست آورد (شامل کلمات عبور هش شده) نمی تواند کلمات عبور اولیه را از روی آن ها بازیابی کند

نموداری برای درک راحت هش ها :



توجه داشته باشید که ...

هش ها دو خصوصیت دارند که باید درباره آن ها بدانید :

یک) الگوریتم های هش معکوس پذیر نیستند .

دو) هرگز دو ورودی متفاوت به یک خروجی یکسان منجر نمی شوند !

در صورتی که هر یک از این دو خصوصیت نقض بشه می گیم الگوریتم شکسته شده است !

مواردی که از هش ها استفاده میکنیم :

الف) تشخیص درستی یک فایل **Verifying file integrity** :

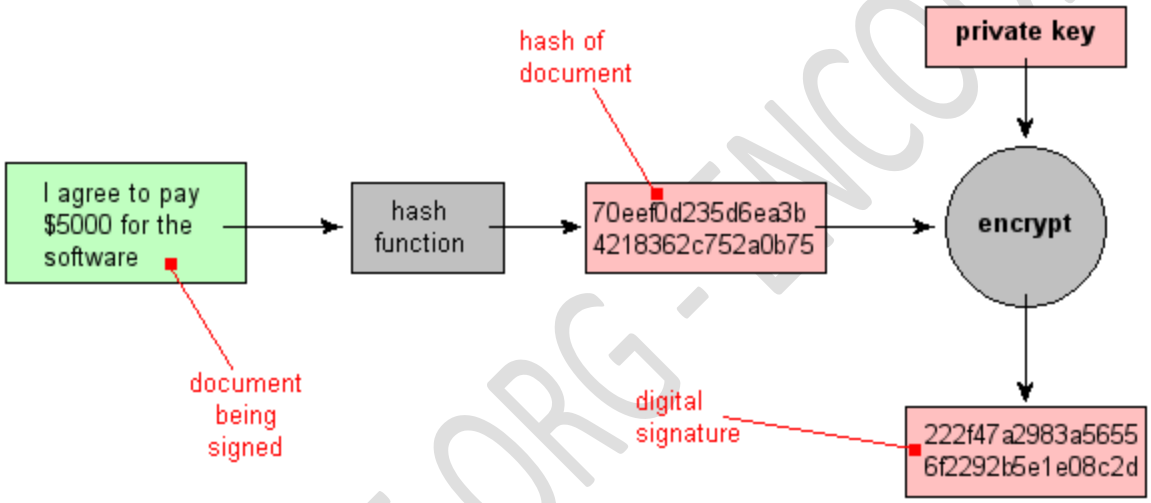
برای مثال زمانی که یک فایل با حجم بالا را دانلود می نماییم می توانیم با به دست آوردن مقدار **MD5** آن فایل توسط دستور **MD5SUM** و مقایسه آن با **MD5** داده شده توسط سایت از درستی فایلمان اطمینان

حاصل کنیم

ب) تبدیل کلمه عبور به هش Hashing Password:

ج) نشانه گذاری اسناد به روش Digitaly (امضا های Digitaly) :

که نحوه انجام ان به وضوح در شکل زیر نشان داده شده است:



انواع مختلفی از الگوریتم های قوی هش کردن برای استفاده در برنامه های کاربردی موجود هستند، محبوب ترین آنها که مورد استفاده برنامه نویسان هستند **MD5** و**SHA-1(Secure hash algorithm)** می باشند.
الگوریتم های قوی تری مانند **SHA-256** و **SHA-512** برای موارد خاص مانند امضاهای دیجیتالی توصیه می گردد ولی برای هش کردن کلمات عبوردر برنامه های امروزی **SHA-1** هنوز سطح امنیت بسیار خوبی را فراهم می کند.

---- لیست هش ها در صفحه بعدی -----

هش های عمومی که زیاد مورد استفاده قرار می گیرند :

md5	d41d8cd98f00b204e9800998ecf8427e
md4	31d6cfe0d16ae931b73c59d7e0c089c0
md2	8350e5a3e24c153df2275c9f80692773
sha1	da39a3ee5e6b4b0d3255bfef95601890afd80709
sha256	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
sha384	38b060a751ac96384cd9327eb1b1e36a21fdb71114be07434c0cc7bf63f6e1da274edebfe76f65fbd51ad2f14898b95b
sha512	cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e
LM	aad3b435b51404eeaad3b435b51404ee
NT	31d6cfe0d16ae931b73c59d7e0c089c0
base_64	
rot_13	

هش های غیر عمومی که برای سازمان های دولتی آماده شده اند و به صورت تجربی بدست آمده و زیاد دیده نمی شوند ! مگر در موارد خاص در صفحه بعدی ...

crc32	00000000
crc32b	00000000
snefru	8617f366566a011837f4fb4ba5bedea2b892f3ed8b894023d16ae344b2be5881
gost	ce85b99cc46752fffee35cab9a7b0278abb4c2d2055cff685af4912c49490f8d
adler32	01000000
ripemd128	cdf26213a150dc3ecb610f18f6b38b46
ripemd160	9c1185a5c5e9fc54612808977ee8f548b2258d31
tiger128,3	24f0130c63ac933216166e76b1bb925f
tiger128,4	4635fff6a778cc243da15c69594e98e7
tiger160,3	24f0130c63ac933216166e76b1bb925ff373de2d
tiger160,4	4635fff6a778cc243da15c69594e98e79451256e
tiger192,3	24f0130c63ac933216166e76b1bb925ff373de2d49584e7a
tiger192,4	4635fff6a778cc243da15c69594e98e79451256e680b4e80
haval128,3	c68f39913f901f3ddf44c707357a7d70
haval128,4	ee6bbf4d6a46a679b3a856c88538bb98
haval128,5	184b8482a0c050dca54b59c7f05bf5dd
haval160,3	d353c3ae22a25401d257643836d7231a9a95f953
haval160,4	1d33aae1be4146dbaaca0b6e70d7a11f10801525
haval160,5	255158cfc1eed1a7be7c55ddd64d9790415b933b
haval192,3	e9c48d7903eaf2a91c5b350151efcb175c0fc82de2289a4e
haval192,4	4a8372945afa55c7dead800311272523ca19d42ea47b72da
haval192,5	4839d0626f95935e17ee2fc4509387bbe2cc46cb382ffe85
haval224,3	c5aae9d47bffcaaf84a8c6e7ccacd60a0dd1932be7b1a192b9214b6d
haval224,4	3e56243275b3b81561750550e36fcd676ad2f5dd9e15f2e89e6ed78e
haval224,5	4a0513c032754f5582a758d35917ac9adf3854219b39e3ac77d1837e
haval256,3	4f6938531f0bc8991f62da7bbd6f7de3fad44562b8c6f4ebf146d5b4e46f7c17
haval256,4	c92b2e23091e80e375dadce26982482d197b1a2521be82da819f8ca2c579b99b
haval256,5	be417bb4dd5cfb76c7126f4f8eeb1553a449039307b1a3cd451dbfdc0fbbe330
whirlpool	19fa61d75522a4669b44e39c1d2e1726c530232130d407f89afee0964997f7a73e83be698b288febcf88e3e03c4f0757ea8964e59b63d93708b138cc42a66eb3

امیدوارم که از این مقاله هم لذت برده باشید

با تشکر

سینا احمدی